

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-271884

(43) 公開日 平成7年(1995)10月20日

(51) Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 F 19/00

G 0 9 C 1/00

H 0 4 L 9/00

9364-5L

G 0 6 F 15/ 30

3 4 0

3 6 0

審査請求 未請求 請求項の数12 F D (全 13 頁) 最終頁に続く

(21) 出願番号 特願平7-49237

(22) 出願日 平成7年(1995)2月15日

(31) 優先権主張番号 1 9 8 8 0 0

(32) 優先日 1994年2月17日

(33) 優先権主張国 米国 (U S)

(71) 出願人 390035493

エイ・ティ・アンド・ティ・コーポレーション

AT&T CORP.

アメリカ合衆国 10013-2412 ニューヨーク
ニューヨーク アヴェニュー オブ
ジ アメリカズ 32

(72) 発明者 マイケル ジョン メリット

アメリカ合衆国、60563 イリノイ、ネイ
パービル、#1329、イロクオイス アベニ
ュー 1101

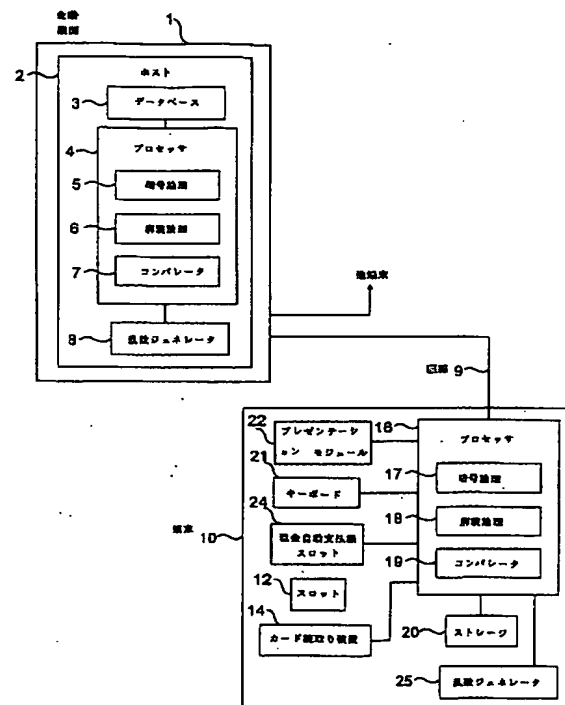
(74) 代理人 弁理士 三保 弘文

(54) 【発明の名称】 端末認証方法

(57) 【要約】

【目的】 トランザクション実行システムで自動窓口端末機のような端末をユーザつまり顧客に対し認証する対顧客端末認証法を提供する。

【構成】 この端末は暗号方式を用い中央ホストにより認証されるが、パーソナル・セキュリティ・フレーズ (P S P) がこの端末からそのホストへ送信される。このP S Pを組み込んだメッセージをこの端末によりその顧客へ通信されそれによりこの端末が正当であることを示す。この顧客がパーソナル識別番号のような何らかの秘密情報をこの端末に入力する前にこの端末をこの顧客に対し認証する。



【特許請求の範囲】

【請求項 1】 トランザクション実行システムでユーザに対し端末を認証する端末認証方法において、

(A) 前記端末に口座情報を受信する口座情報受信ステップと、

(B) 前記口座情報を発行した機関と関係付けられたホストと通信回線を経て接触する接触ステップと、

(C) 前記端末から前記ホストへ前記口座情報の少なくとも一部を送信する口座情報送信ステップと、

(D) 前記ホストから前記端末へ前記口座に対応したパーソナル・セキュリティ・フレーズを送信するパーソナル・セキュリティ・フレーズ送信ステップと、

(E) 前記端末において前記ユーザに対し前記パーソナル・セキュリティ・フレーズを組み込んだメッセージを通信する通信ステップと、を有し、前記ステップは前記端末に前記ユーザがいずれかの秘密または機密の情報を入力するステップに先だって行うことを特徴とする端末認証方法。

【請求項 2】 前記 (E) ステップは、前記端末に結合したプレゼンテーション・モジュールに前記パーソナル・セキュリティ・フレーズを表示する表示ステップを有することを特徴とする請求項 1 に記載の方法。

【請求項 3】 前記 (D) ステップは、複数の英数字、複数のワード、ビデオ画像、ビデオ画像のシーケンスのいずれかの形を持つパーソナル・セキュリティ・フレーズを送信するステップを有することを特徴とする請求項 2 に記載の方法。

【請求項 4】 (F) 前記パーソナル・セキュリティ・フレーズ送信ステップは録音の形を持つパーソナル・セキュリティ・フレーズを送信するステップと、

(G) 前記パーソナル・セキュリティ・フレーズを組み込んだメッセージを通信する前記通信ステップは前記端末に結合したプレゼンテーション・モジュールを経て前記パーソナル・セキュリティ・フレーズを音声で送信するステップとを更に有することを特徴とする請求項 1 に記載の方法。

【請求項 5】 前記端末は自動窓口端末機であることを特徴とする請求項 1 に記載の方法。

【請求項 6】 前記ステップは前記自動窓口端末機にパーソナル識別番号を前記ユーザが入力するステップに先だって行うことを特徴とする請求項 5 に記載の方法。

【請求項 7】 前記 (E) ステップは、さらに、前記ユーザが前記パーソナル・セキュリティ・フレーズを前記ユーザ自身のものと認める場合にのみ前記自動窓口端末機に前記ユーザのパーソナル識別番号を入力するよう前記ユーザに命令する命令ステップを有することを特徴とする請求項 6 に記載の方法。

【請求項 8】 さらに、(H) 前記端末を前記ホストに対し認証する端末認証ステップを有し、前記 (H) ステップは、前記 (D) ステップに先だって行うことを特徴

とする請求項 1 に記載の方法。

【請求項 9】 前記 (E) ステップは、前記端末に結合したプレゼンテーション・モジュールで前記パーソナル・セキュリティ・フレーズを表示するステップを有することを特徴とする請求項 8 に記載の方法。

【請求項 10】 前記 (D) ステップは、複数の英数字、複数のワード、ビデオ画像、ビデオ画像のシーケンスのいずれかの形を持つパーソナル・セキュリティ・フレーズを送信するステップを有することを特徴とする請求項 9 に記載の方法。

【請求項 11】 前記 (H) ステップは、

(H1) 前記自動窓口端末機と関係付けられた通し番号を前記ホストに送信する通し番号送信ステップと、

(H2) 前記ホストにおいて第 1 の乱数を生成する第 1 の乱数生成ステップと、

(H3) 前記第 1 の乱数を前記ホストから前記自動窓口端末機へ送信する第 1 の乱数送信ステップと、

(H4) 前記自動窓口端末機に蓄積した安全保障の第 1 のキーを用いて、前記通し番号と前記第 1 の乱数と第 1 の指示コードの暗号を前記自動窓口端末機において計算する第 1 のキー使用暗号計算ステップと、

(H5) 前記自動窓口端末機から前記ホストへ安全保障の前記第 1 のキーを用いて前記通し番号と前記第 1 の乱数と前記第 1 の指示コードの前記暗号を送信する暗号送信ステップと、

(H6) 前記ホストに蓄積した安全保障の第 2 のキーを用いて前記通し番号と前記第 1 の乱数と前記第 1 の指示コードの暗号を前記ホストにおいて計算する第 2 のキー使用暗号計算ステップと、

(H7) 前記第 2 のキーを用いて計算した前記通し番号と前記第 1 の乱数と前記第 1 の指示コードの前記暗号と、前記第 1 のキーを用いて計算した前記通し番号と前記第 1 の乱数と前記第 1 の指示コードの前記暗号を、前記ホストにおいて比較する暗号比較ステップと、

(H8) 前記第 2 のキーを用いて計算した前記通し番号と前記第 1 の乱数と前記第 1 の指示コードの前記暗号と、前記第 1 のキーを用いて計算した前記通し番号と前記第 1 の乱数と前記第 1 の指示コードの前記暗号が等しいことを、前記ホストにおいて検証する検証ステップを有することと特徴とする請求項 8 に記載の方法。

【請求項 12】 前記 (H) ステップは、

(H1) 前記自動窓口端末機において第 2 の乱数を生成する第 2 の乱数生成ステップと、

(H2) 前記第 2 の乱数を前記自動窓口端末機から前記ホストへ送信する第 2 の乱数送信ステップと、

(H3) 前記第 1 のキーを用いて前記通し番号と前記第 2 の乱数と前記第 1 の指示コードと異なる第 2 の指示コードの暗号を前記ホストにおいて計算する第 1 のキー使用暗号計算ステップと、

(H4) 前記ホストから前記自動窓口端末機へ前記第 1

3

のキーを用いて前記通し番号と前記第2の乱数と前記第2の指示コードの暗号を送信する暗号送信ステップと、

(H5) 前記第2のキーを用いて前記通し番号と前記第2の乱数と前記第2の指示コードの暗号を前記自動窓口端末機において計算する第2のキー使用暗号計算ステップと、

(H6) 前記第2のキーを用いて計算した前記通し番号と前記第2の乱数と前記第2の指示コードの前記暗号と、前記第1のキーを用いて計算した前記通し番号と前記第2の乱数と前記第2の指示コードの前記暗号を、前記自動窓口端末機において比較する暗号比較ステップと、

(H7) 前記第2のキーを用いて計算した前記通し番号と前記第2の乱数と前記第2の指示コードの前記暗号と、前記第1のキーを用いて計算した前記通し番号と前記第2の乱数と前記第2の指示コードの前記暗号が、等しいことを前記自動窓口端末機において検証する検証ステップとを更に有することを特徴とする請求項8に記載の方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、トランザクション実行システムに係り、特にこのトランザクション実行システムには中央ホストがあつて取引処理、例えば、現金の払出または口座間預金振替のようなトランザクションを実行できる遠隔端末と通信しトランザクションを実行するトランザクション実行システムの要素をユーザつまり顧客に対し認証する認証方法に関する。

【0002】

【従来の技術】トランザクション端末、例えば、何時でも動作可能な自動窓口端末機(ATM)は、無人場所で現金の払出や他の金融取引処理のトランザクションの要望を満たすためこの利用は広く受け入れられてきた。ATMの便利なことからこのような処理は一般大衆に非常に普及した。さらに、小売商品販売店のオーナーが知ったことというのは、ATMの見込める場所は顧客をその小売場所に引寄せ顧客が現金購入するという件数が増加したことである。そのためATM場所は銀行のような関連金融機関の場所から遠く離れた場所である場合が多い。このようなATMや他のトランザクション端末の分布システムからいくつかの複雑なセキュリティ問題が生じた。この金融業界は特にこのセキュリティ問題に関心を持っている。

【0003】ATMを用いる、例えば、電子預金振替

(EFT)システムでは、トランザクションを実行するために機器上でそのユーザの署名、ただしこれは容易に偽造可能であるが、これを通常必要としない。それより、そのユーザの秘密のパーソナル識別番号(PIN)とプラスチックの銀行カードつまりトランザクション・カードがこのEFTシステムに対しそのユーザを識別し

4

検証するための役目をする。このPINは、例えば、4桁の番号でできる。通常はこのユーザがその銀行カードをこのATMのスロットに挿入しその後このATMがそのユーザにユーザのPINの入力をプロンプトする。次にこのユーザはそのPINをそのATMに付随するキーボードに入力すると、このATMは次にそのPINをこのATMに結合したデータベースの蓄積情報と比較する。

【0004】この比較で適切なPINが入力されたことを示す場合にのみそのトランザクションは進むことができる。いくつかのセキュリティ問題は、正当な顧客のPINや他の口座情報を得た不正者の場合に生ずる。この状況に特に関心が払われる理由は、この不正者がその正当な顧客の専用口座の蓄積情報にアクセスできたその口座の蓄積預金にアクセスできるからである。この問題に対応して、この金融業界はPIN番号と銀行カードの不正使用に対抗するためいろいろな方法を適用してきた。例えば、このユーザがそのPINをそのATMに付随のキーボードに入力してしまうとそのPINを符号化するため暗号動作を使用することが知られている。このような対抗法により不正者がネットワーク・リンクで送られるメッセージをモニタしたりそのためPIN情報を入手したりできぬようにする。

【0005】ところが最近、PINや他の口座情報を入力するため不正者は高度で精巧な方法を使用するようになってきた。このような不正な方法の一例に偽造ATMを商店街や他の公共の場所に設置する例がある。この偽造端末機は、顧客がその銀行カードつまりトランザクション・カードを挿入しそのPINを入力しても現金の払出はしない。しかし、この偽造端末機は、この端末機で行われた現金払出の無効な試行でその顧客が入力したカード口座番号やPINを保持し記録する。そしてこの記録情報を用いて実際の銀行カードのアクションを活動化する偽造プラスチック・カードの作成を可能にする。その偽造端末機が記録したPINと共にこの偽造カードを正当なATMで用いて他人の銀行口座の蓄積預金の振替または引出が可能となる。

【0006】以上説明した例のようなスキームからATMまたは他のトランザクション端末をユーザまたは顧客に対し認証する認証法が必要で、それも秘密または機密の情報をそのATMまたは他のトランザクション端末にそのユーザまたは顧客が提供する前に、認証法が必要である。通信システムにおいて暗号方式を用いてハードウェア要素を互いに認証する認証方法は既知である。この認証方法の一例に、米国特許第4,799,061号、“安全保障要素認証システム”、アブラハム＝(Abraham)ら、に開示の方法を挙げることができる。しかしこれらの方法は、その要素をユーザつまり顧客に対して認証しない。ユーザに機密情報を入力するよう要求する端末をユーザに対し認証する問題は以前にも認めら

5

れており、いくつかの参考文献の中に下記のような解決法の一例が知られている。

【0007】それは、別個のパーソナル・ポータブル端末デバイスをそのユーザに提供する方法である。米国特許第4、529、870号、“暗号識別、金融トランザクションおよび信用証明デバイス”では、例えば、次のような暗号装置を提供する。この暗号装置は、外部コンピュータ・システムに対しその身元を明らかにするためその所有者により使用され、そして外部システムと種々の金融トランザクションを実行でき、また外部システムに対し種々の信用証明を提供できる。一実施例では、この装置は、暗号デバイスとパーソナル端末デバイスに分離可能である。この装置の所有者はそのパーソナル端末デバイスをおそらくよく制御し、機密データが業者の販売時点端末のような端末に不当に保持されないようにする。しかし、このようなデバイスにも追加ハードウェアをそのカード形状デバイスに組込む必要がありまたこのデバイスや他のシステム要素が通信できるよう追加変更が必要である。

【0008】

【発明の解決しようとする課題】このような追加や変更の必要の無い自動窓口端末機のような端末をユーザつまり顧客に対し認証する有効な対顧客端末認証法が要望されている。

【0009】

【課題を解決するための手段】本発明は、トランザクション実行システムに以下に説明する認証方法を提供し前記課題を解決しこの分野の技術的進歩を遂げる。すなわち本発明は、トランザクション実行システムには中央ホストがあつて、例えば、現金の払出または口座間預金振替のトランザクションを実行できる遠隔端末と通信しトランザクションを実行するシステムの要素をユーザつまり顧客に対し認証する認証方法を提供する。本発明の認証方法には次のステップがある。すなわち、端末において口座情報を受信する口座情報受信ステップと、前記口座情報を発行した機関に関係付けられたホストと通信回線を経て接触する接触ステップと、前記端末から前記ホストへ前記口座情報の少なくとも一部を送信する送信ステップと、前記ホストから前記端末へ前記口座に対応するパーソナル・セキュリティ・フレーズを送信するパーソナル・セキュリティ・フレーズ送信ステップがある。

【0010】さらに本発明の認証方法には、前記端末において前記ユーザに対し前記パーソナル・セキュリティ・フレーズを組込んだメッセージを通信する通信ステップがある。さらに本発明の方法では、前記ステップは前記ユーザがいずれかの秘密または機密の情報を入力するステップに先だつて生ずるものである。さらに本発明の認証方法の特徴と利点は以下の詳細な説明と添付参照図面から明白である。

【0011】

6

【実施例】図1は本発明に特に好都合なトランザクション実行システムを示す図である。機関1は例えば、銀行のような金融機関である。この銀行1にはホスト2がある。このホスト2にはデータベース3とプロセッサ4がある。このプロセッサ4には暗号論理5と解読論理6とコンパレータ7がある。またこのホスト2には乱数ジェネレータ8がある。端末10は、例えば複数の地理的に分布した自動窓口端末機(ATM)の中の1個のATMである。このATMは例えば電話回線のような通信回線9によりその銀行のホスト2に結合する。このATM10には、顧客が挿入した銀行カードを受入れたり戻したりするスロット12があり、さらにこのカードに蓄積した情報を読み取る手段のカード読取り装置14がある。

【0012】このカード読取り手段14はプロセッサ16に結合する。このプロセッサ16には暗号論理17と解読論理18とコンパレータ19がある。乱数ジェネレータ25もまたこのプロセッサ16に結合する。またこのATM10には情報またはデータを蓄積する手段のストレージ20があり、このストレージ20はプロセッサ16に結合する。さらにこのATM10にはまたキーボード21とプレゼンテーション・モジュール22があり、これらはプロセッサ16に結合する。このプレゼンテーション・モジュール22には例えば、次のような表示手段のある表示画面を挙げることができる。この表示手段は静止画像または画像シーケンス、例えば、ビデオ画面をビデオ・カードで表示する手段である。このプレゼンテーション・モジュール22にはまた音声通信手段があり、これは音声カードで例えば、スピーカのように音声を通信する手段である。

【0013】最後にこのATM10には現金を自動支払する第2のスロット24があり、これもまたプロセッサ16に結合する。さらに図1には図示していないが、この銀行ホスト2に結合できる追加端末がある。このATM10のような新規端末が図1に示すトランザクション実行システムの一部としてオンライン状態に入ると、この銀行1はそれに通し番号のSと暗号キーのKを割当てる。この通し番号のSは例えば、4桁または他の適当な長さの番号とすることができる。この暗号キーのKは安全保障暗号スキームに使用できるものである。Kには例えば、56ビット・データ暗号規格(DES)キーを挙げることができ、これは例えば、“データ暗号規格”、FIPS、Pub. 46、米国標準規格局(1977年1月)、に記載のような暗号システムに使用のものである。

【0014】ここに参照する前記報告、関連報告および特許を引例とし説明を続ける。この通し番号と暗号キーはそのATMストレージ手段20と銀行ホスト2の両者に蓄積される。この銀行1で顧客が口座を得よう登録するとこの顧客に口座番号が割当てられる。この銀行1はこの顧客にプラスチックのトランザクション・カード

すなわち銀行カードを通常供与するが、このカードには適当な口座情報を含む磁気ストリップがある。この情報にはこのカードを発行した銀行を識別する銀行識別番号とこの顧客の口座番号と顧客名を通常含むが、他の情報もまた含むことができる。(このトランザクション・カードにはまた例えば、米国特許第4、795、898号に記載のようなスマート・カードを挙げることができる。)次にこの顧客は例えば、4桁番号のパーソナル識別番号(PIN)を選択しまたはこの顧客にそれが割当てられる。

【0015】このPINは機密が保持されこのカードの使用許可の無い者にはそれを伝えないよう一般に意図されている。本発明の方法ではこの顧客はまたパーソナル・セキュリティ・フレーズ(PSF)を選択しまたはこの顧客にそれが割当てられる。このパーソナル・セキュリティ・フレーズにはワードつまり英数字のいずれかの組合わせを用いることができるが、その全体の長さは所定の長さ以下でその特定の顧客が比較的記憶または認識し易いフレーズが好ましい。ただしこのPSFは英数字に限定するものではない。このPSFは電子的に伝送可能な静止画または画像シーケンスでもよい。同様にこのPSFは録音音声の形でよい。英数字のある組合わせの形を取るPSFの場合と同様にビデオPSFまたは音声PSFもその顧客が比較的記憶または認識し易いものが好ましい。

【0016】次にこのPSFは他の情報と共にこの銀行1の係員によりそのホスト2に入力されるが、この他の情報にはその顧客名やその顧客の口座番号やその顧客のPINがある。このPINそれ自身はそのホスト2に蓄積されず、むしろこのPINの暗号化バージョンやまたはハッシュ・バージョンを例えば、ワンウェイ・ファンクションを用いて蓄積する。このワンウェイ・ファンクションは従来周知であり、これについては例えば、次に挙げる報告に記載があり参照のこと。エイ・エバンス(A. Evans)ら、“コンピュータにおける秘密不要ユーザ認証スキーム”、Comm. ACM、第17巻、8号、437-442頁(1974年)である。このPSFは暗号化の形で蓄積できるがその必要は無い。図2にこの銀行のデータベース3へのエン트리200例を示す。

【0017】ここで説明の便宜上次のように仮定する。この顧客名はミスタ・デービッドB. スミス、その口座番号は“XYZ”、そのPINは“1234”、およびそのPSFは“家でチャリティが始る”とする。こうするとこの銀行のデータベース3のエン트리200に下記の入力がある。氏名=ミスタ・デービッドB. スミス、口座=XYZ、PIN=OW(1234)、PSF=家でチャリティが始る、で図2に示す通りである。ここで“OW(1234)”は特定のワンウェイ・ファンクションを用いたPINの暗号化形である。図3に本発

明の認証法による認証プロセスの流れ図を示し、これを参照し説明を続ける。

【0018】顧客、ここでは例えば、ミスタ・デービッドB. スミスが、例えば、ATM10の端末を用いて金融トランザクションの実行を所望する場合、ステップ300に示すようにこの顧客はその銀行カードをそのATM10のスロット12に挿入する。ステップ305において、このATMはこのカードからその口座情報を読み取る。前述のようにこの情報には通常この顧客名のデービッドB. スミスと口座番号のXYZがある。当然のことであるが、この顧客がその端末に端末機読み取り可能カードを挿入しないで手動でその端末にその口座情報を入力するようなトランザクション実行システムも可能である。次にステップ310において、このATM10は通信回線9でその銀行ホスト2と接触する。ステップ315において、このATM10とこの銀行ホスト2は、以下に詳しく説明するツーウェイ・チャレンジレスポンス(two-way challenge-response)に参加する。

【0019】さらに具体的に説明すると、ステップ320において、このATM10はこの銀行ホスト2に対し正当であることを確認するようその身元を明らかにするつまり身元認証する。ステップ340において、この銀行ホスト2はこのATM10に対しこのATM10は正当な銀行に接触したことを確認するようその身元を明らかにするつまり身元認証する。このATMと銀行ホスト間に生ずるツーウェイ・チャレンジレスポンスは一方が他方に対しその身元を認証できる限り特定の形に限定するものではない。通信システムにおいて要素を認証する認証方法は既知である。本発明の一実施態様ではこの認証スキームは暗号方式を用いてそれぞれが適切なキーを持つかその正否を決める。特に各要素はその他方がまさにその等しい暗号キーを保持しているかそれを検証する。

【0020】このような認証スキームの一例に前記米国特許第4、799、061号に開示のスキームを挙げることができる。銀行ホストが保持するキーとATMに蓄積されたキーの身元を明らかに検証する身元検証の好ましい実施例を図4に示す。説明の便宜上相互に検証しようとする端末とホストはそれぞれこのATM10とホスト2であると仮定する。さらに説明の便宜上このホストは暗号キーK1をこのATMは暗号キーK2を持つと仮定する。当然のことであるが、この銀行とATMが正当である場合にはこの2個のキーのK1とK2は等しく、それらはキーKに等しいと定義する。参照する図4ではステップ321に示すようにこのATM10はその通し番号Sを銀行ホスト2へ送信する。この情報は暗号形では送信しない。

【0021】次にステップ322において、このホスト2はその乱数ジェネレータ8を用いて第1の乱数CAを

生成する。次にステップ323において、このホスト2はそのATM10へこの乱数CAを送信する。またこの情報は暗号形で送信する必要はない。ステップ325において、このATM10は、そのキーK2と暗号論理17を用いてSとCAと第1の指示コードの暗号eK2

(S、CA、0)を計算する。この指示コードは指示ビット“0”で示したが、他の指示コードも同様に使用できる。またステップ326において、このATM10はまたその乱数ジネレータ25を用いて第2の乱数CBを生成する。次にステップ327において示すように、このATM10はCBとそのSとCAと第1の指示コードの暗号をホスト2に送信する。

【0022】ステップ330において、ただしこのステップ330はそのステップ325ないし327に先だつて、またはステップ325ないし327と同時に、さらにまたはステップ325ないし327に続いて、のいずれかで生ずることができるステップであるが、このステップ330において、このホスト2はそのキーK1と暗号論理5を用いてSとCAと第1の指示コードの暗号eK1(S、CA、0)を計算する。次にステップ331に示すように、ステップ327、330に続きこのホスト2はコンパレータ7においてSとCAとその指示コードのホストの暗号を同じ情報のATMの暗号と比較する。この暗号値が等しくない場合には、ステップ332において、このホスト2はそのATM10との間に設定された通信回線を切断する。またステップ335に示すように、このホスト2はそのトランザクション実行システムに不正端末が結合された可能性があることをシステム・オペレータに警告する。

【0023】これに反しこの暗号値が等しいことをこのホスト2が検証した場合、ステップ336で示すように、このATM10は認証される。ステップ345において、このホスト2はそのキーK1と暗号論理5を用いてSとCBと第1の指示コードと異なる第2の指示コードの暗号eK1(S、CB、1)の計算に進む。次にステップ347において、このホスト2はそのSとCBと第2の指示コードの暗号をそのATM10に送信する。ステップ350において、ただしこのステップ350はステップ345、347に先だつて、またはステップ345、347と同時に、さらにまたはステップ345、347に続いて、のいずれかで生ずることができるステップであるが、このステップ350において、このATM10はそのキーK2と暗号論理17を用いてSとCBと第2の指示コードの暗号eK2(S、CB、1)を計算する。

【0024】次にステップ351で示すように、このATM10はそのコンパレータ19を用いてそのSとCBと第2の指示コードの暗号を同じ情報のホストの暗号と比較する。この暗号値が等しくない場合には、ステップ352において、このATM10はそのホスト2との間

に設定された通信回線を切断する。次にステップ353に示すように、そのプレゼンテーション・モジュール22でエラー・メッセージを表示し、ステップ354に示すように、スロット12を経てその顧客のカードをリターンする。またステップ355において、このATM10はそのトランザクション実行システムに不正なホストが結合された可能性があることをシステム・オペレータに警告する。これに反して、その暗号値が等しいことをこのATM10が検証した場合、ステップ356に示すように、このホスト2は認証される。

【0025】このステップ356でこの銀行ホスト2とATM10間のツーウェイ・チャレンジレスポンスは完了し、ステップ359において示すように、本発明の方法は図3のステップ360に続く。ここで付記すべきことは前記ツーウェイ・チャレンジレスポンスには種々の変形が可能である。例えば、ステップ330ないし331の代りに、ステップ327においてこのホスト2はそのATM10から受信した暗号情報をそのキーK1と解読論理6を用いて解読し、SとCAと第1の指示コードを検索したかそれを検証する。それらが検索された場合には、ステップ336において、このホスト2は認証される。同様の変形がこのステップ350ないし351について可能である。具体的に説明すると、ステップ347においてこのATM10はそのホスト2から受信した暗号情報をそのキーK2と解読論理18を用いて解読する。

【0026】そしてSとCBと第2の指示コードを検索したかそれを検証する。それらが検索された場合には、ステップ356におけるようにこのホスト2は認証される。図3に戻り説明を続ける。ステップ360において、このATM10はその口座情報をこの銀行ホスト2へ送信する。このホスト2は、そのデータベース3からこの顧客の口座に対応するエントリ200に含まれた情報を検索し、ステップ370において、このホスト2はそのATM10へこの顧客のPSP“家でチャリティが始る”を送信する。またここで以下に説明する利用のためそのワンウェイ・ファンクションで暗号化したこの顧客のPINをそのATM10へ送信できる。次にステップ380において、この顧客のPSPを組込んだメッセージを通信してこのATM10はその身元をこの顧客に対し認証する。

【0027】例えば、このATM10はそのプレゼンテーション・モジュール22で次のようなメッセージを表示する。例えば、「スミスさん、おはようございます。スミスさんのパーソナル・セキュリティ・フレーズは“家でチャリティが始る”です。これが正しい場合はスミスさんの4桁のパーソナル識別番号を入力してください。」である。この顧客のミスタ・スミスがこのPSPを自分自身のPSPであると認識する場合にのみステップ390においてこの顧客のミスタ・スミスは自分のP

INをそのキーボード21に入力する。このPSPが静止画像または画像シーケンスの形である場合、同じようなメッセージはこの顧客とこの英数字PSPをそのビデオPSPにより代えて通信する。

【0028】同様に、このPSPが録音音声の形の場合、同じようなメッセージはこの顧客とそのプレゼンテーション・モジュール22を経て音声で通信された音声PSPによりこの英数字PSPを代えて通信する。好ましい実施例では、このATM10とホスト2が相互に認証してしまうと、後続するこれらの間の通信はすべてこれら通信の安全を保障するため暗号形で送信される。このATM10とホスト2は、例えば、その共用キーのKを用いて継続が可能である。または、このATM10とホスト2は、従来周知の方法でなんらか他の機構によりセッション・キーを取決めたりまたはその回線9の安全を保障したりすることができる。ここでは説明の便宜上このATM10とホスト2はそのキーKを継続使用すると仮定する。

【0029】またここで不正ユーザによる応答アタックを回避するためランザクション識別子を入れる。例えば、このランザクション識別子はそのステップ322またはステップ326で生成した乱数のなかの一つを使用することができる。またはなんらか他の適当なランザクション識別子の使用も可能である。ここでは説明の便宜上このランザクション識別子として乱数CAを使用すると仮定する。本発明の好ましい実施例では図5に示すように、ステップ501においてこのATM10は暗号論理17とそのキーKを用いてこの顧客名とその口座番号とこの乱数CAを含む口座情報を暗号化し、ステップ503において、この暗号化口座情報をそのホスト2へ送信する。

【0030】この口座情報の暗号形を受信すると、ステップ505において、このホスト2は解読論理6とその共用キーKを用いてこの暗号化口座情報を解読する。図5においてはこの共用キーKを用いる暗号解読を項eK-1で表す。次にステップ507において、このホスト2はこの顧客の口座に対応するエントリ200に含まれた口座情報をそのデータベース3から検索する。ステップ509において、このホスト2は暗号論理5とその共用キーKを用いてこの顧客のPSPとCAを暗号化する。次にステップ511に示すように、このホスト2はそのATM10へこの暗号化PSP情報を送信する。この暗号化PSP情報を受信すると、ステップ513において、このATM10は解読論理18を用いてこの暗号化PSP情報を解読する。

【0031】本発明の方法は前記ステップ380、390に示したように進むが、ここでは便宜上図5においてステップ515、516で再示した。またこのATM10がこの顧客のPSPをこの顧客に通信してこの顧客に対しその身元を明らかにするつまり身元認証した後のみ

この顧客はそのキーボード21上にこの顧客のPINを入力する。この顧客がそのPINを入力してしまうと、このATM10はそのPINの処理を従来周知の標準的な方法の中のいずれかの方法にしたがって行いユーザを認証する。例えば、このATM10はそのPINを暗号形でこのホスト2へ送信する。次にこのホストは有効なPINが入力されたことを検証しこのATMにこのランザクションを進めるよう指示する。または、端末10のような新端末をオンライン状態にすると、この銀行1はまたこれにそのワンウェイ・ファンクションを蓄積する。

【0032】この状況においては図3のステップ370または図5のステップ511において、このPINは、そのワンウェイ・ファンクションで暗号化されて、このATM10へこの顧客のPSPと共に送信される。図3のステップ390または図5のステップ516において、この顧客がそのPINを入力してしまうと、このATM10はこれをその内蔵ワンウェイ・ファンクションを用いて暗号化しその結果をこの銀行ホストから受信した値と比較する。それらが等しい場合にはこのATM10はこのランザクションを進ませる。以上本発明の説明は、一つの銀行を取上げ、この銀行がそれ自身の銀行カードを発行しその銀行ホストに結合する複数のATMで利用する場合について行ったが、さらに本発明は次のような交換システムでも利用可能である。

【0033】それは、複数の銀行がそれら自身のそれぞれのATMにおいてその他の銀行が発行したカードも引受けることを合意した交換システムであり、ここでも本発明は適用可能である。さらに、本発明の以上の説明はATMで行ったが、他の種類の端末でも本発明は適用可能である。例えば、業者売場の販売時点の端末でこれが顧客つまりユーザに機密情報を入力するよう要求する端末も本発明の適用可能な端末として挙げることができる。さらにまた、以上の説明は、本発明の一実施例に関するもので、この技術分野の当業者であれば、本発明の種々の変形例がさらに考え得るが、それらはいずれも本発明の技術的範囲に包含される。

【0034】

【発明の効果】以上述べたごとく、本発明の方法では従来法のようにカード形状デバイスにハードウェアの追加など厄介な変更を必要とせずさらに端末を有効に認証して機密データが例えば業者売場の販売時点端末のような端末に不当に保持されることもなく本発明により従来法に比し簡単で有用な対顧客端末認証法がランザクション実行システムに提供でき安全保障の点で大きく向上する。

【図面の簡単な説明】

【図1】本発明の方法が特に好都合であるようなランザクション実行システムの例を示すブロック図である。

【図2】本発明の方法のデータベース・エントリ例を示

10

20

30

40

50

す図である。

【図 3】本発明の方法による認証プロセスのステップを示す流れ図である。

【図 4】本発明の方法により相互に端末とホストを認証する好ましい実施例のステップを示す流れ図である。

【図 5】本発明の方法により端末とホスト間の通信交換の好ましい実施例のステップを示す流れ図である。

【符号の説明】

- 1 (金融) 機関
- 2 ホスト
- 3 データベース
- 4 プロセッサ
- 5 暗号論理
- 6 解読論理
- 7 コンパレータ

8 乱数ジェネレータ

9 通信回線

10 端末 (自動窓口端末機 (ATM))

12 スロット

14 カード読取り装置

16 プロセッサ

17 暗号論理

18 解読論理

19 コンパレータ

10 20 ストレージ

21 キーボード

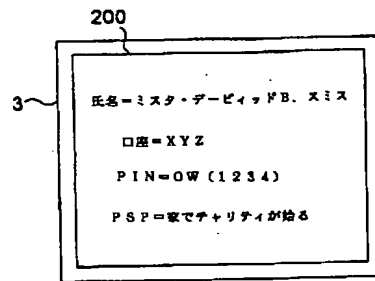
22 プレゼンテーション・モジュール

24 スロット (現金自動支払機)

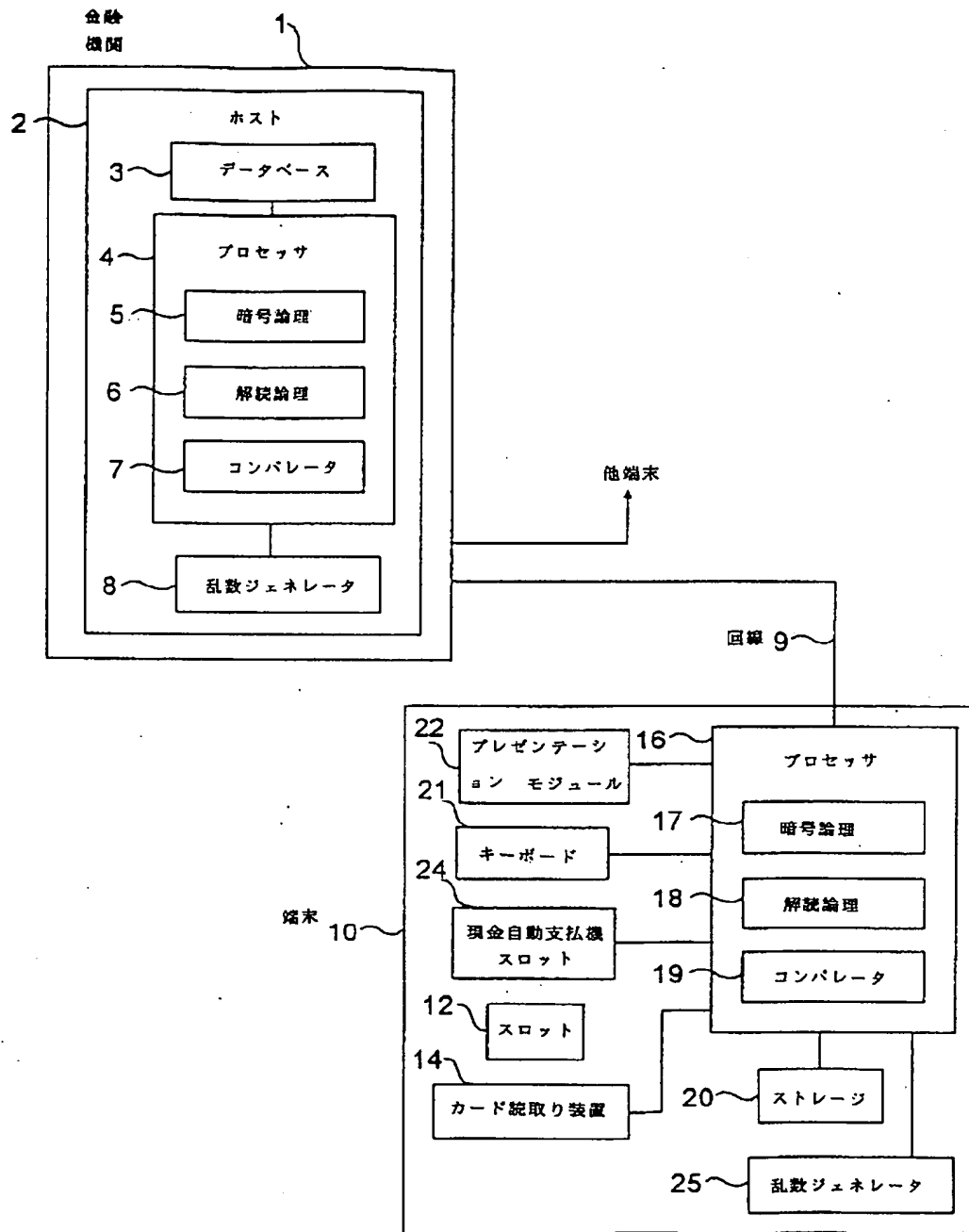
25 乱数ジェネレータ

200 データベース・エントリ

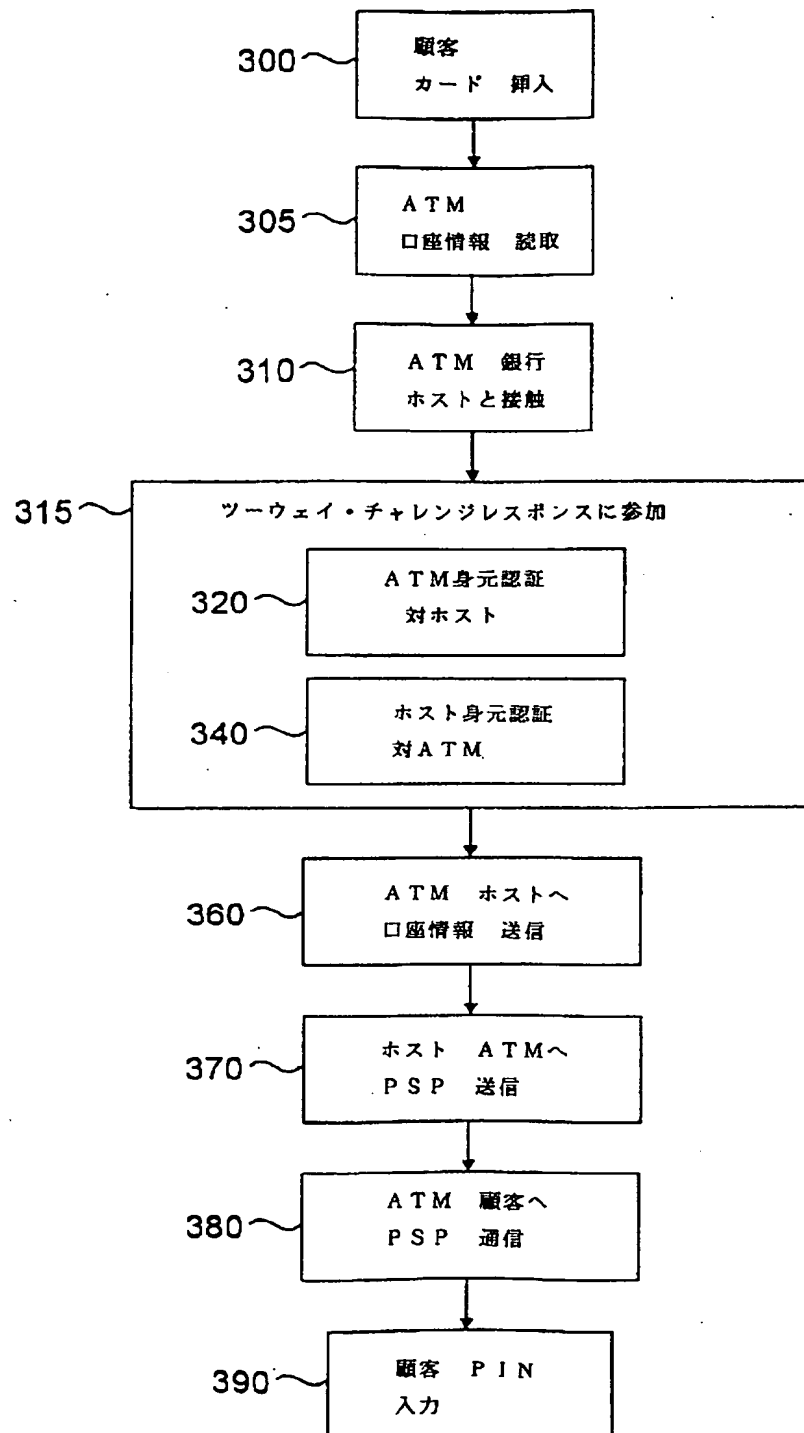
【図 2】



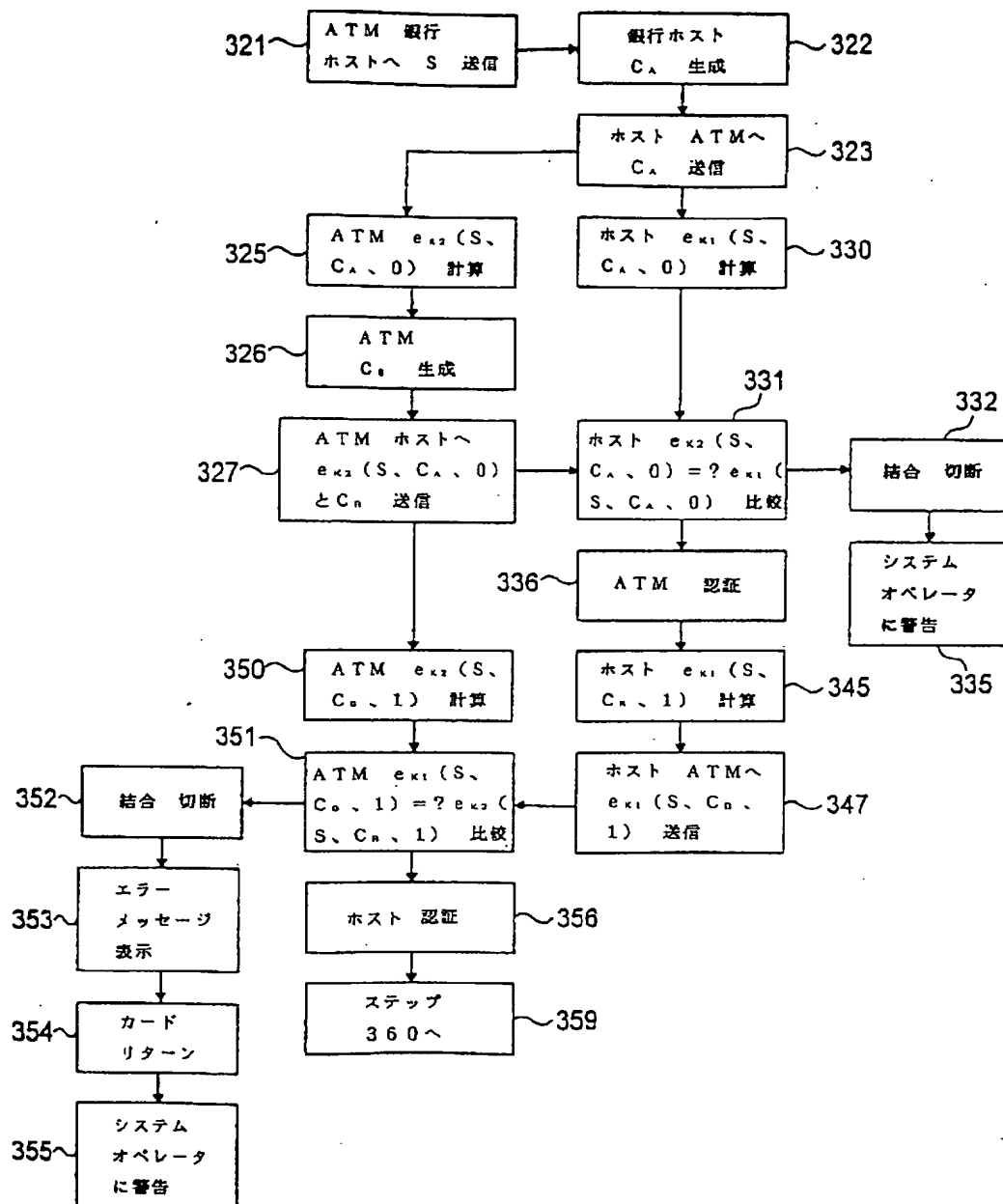
【図 1】



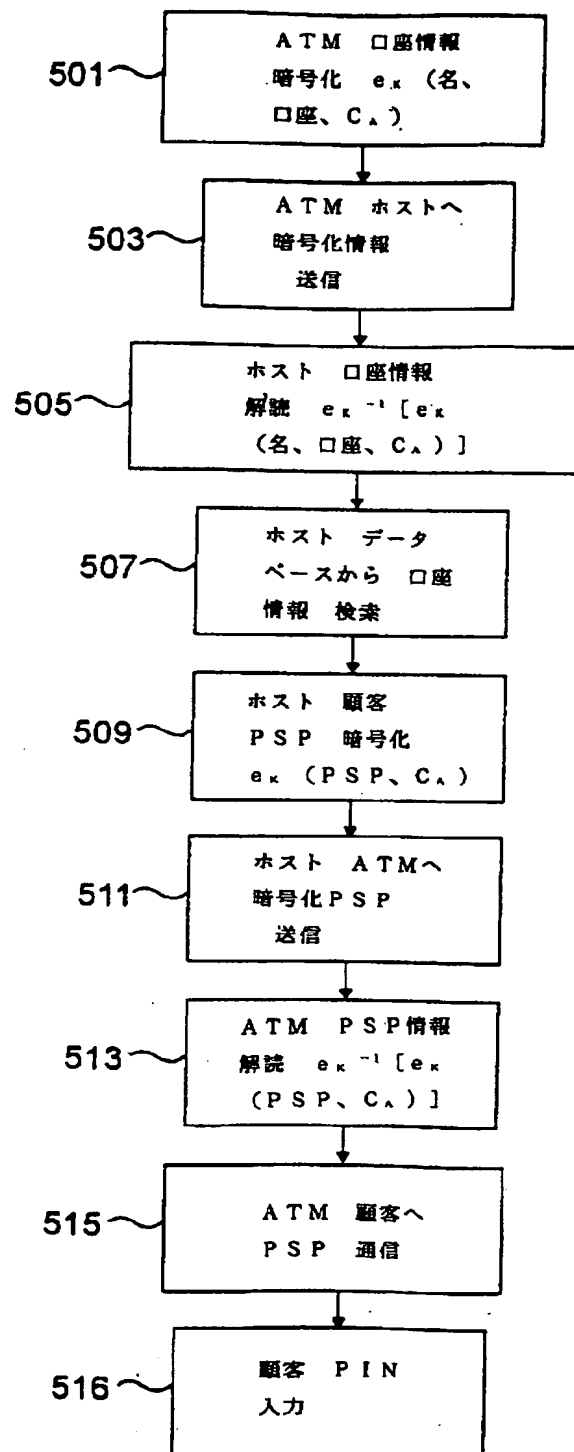
【図 3】



【図 4】



【図 5】



フロントページの続き

(51) Int. Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

H O 4 L 9/10

9/12

H O 4 L 9/00

Z